# UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TENNESSEE AT KNOXVILLE

UNITED STATES OF AMERICA

v.

Case No. 3:21-CR-38

BENJAMIN ALAN CARPENTER a/k/a "Abu Hamza"

Judges Crytzer / Poplin

# GOVERNMENT'S MOTION FOR A PRETRIAL CONFERENCE PURSUANT TO 18 U.S.C. APP. III, (CIPA) SECTION 2

The United States of America, by Francis M. Hamilton III, Acting United States Attorney for the Eastern District of Tennessee, hereby moves the Court to hold a pretrial conference, pursuant to Section 2 of the Classified Information Procedures Act, 18 U.S.C. App. III ("CIPA"). Because the Government anticipates that issues regarding the discovery of classified information will arise during this case, the Government respectfully requests the Court convene a pretrial conference to consider matters relating to such classified information pursuant to Section 2 of CIPA.

## OVERVIEW OF CIPA<sup>1</sup>

CIPA was enacted in 1980 to enable courts to evaluate potential classified information issues in criminal cases before jeopardy attaches. "The Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, provides a set of procedures for federal courts to follow when the government seeks to protect classified information from disclosure." *United States v. Amawi*, 695 F.3d 457, 468 (6th Cir. 2012). CIPA's fundamental purpose is to "harmonize a defendant's

<sup>&</sup>lt;sup>1</sup> The provisions of CIPA which may be relevant to this case are discussed in this Motion. Sections 3 (Protective Orders), 5 (Notice of Defendant's Intention to Disclose Classified Information), and 6 (Procedures for Cases Involving Classified Information) are not relevant to this case.

right to obtain and present exculpatory material [at] trial and the government's right to protect classified material in the national interest." *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996). It "evidence[s] Congress's intent to protect classified information from unnecessary disclosure at any stage of a criminal trial." *United States v. Apperson*, 441 F.3d 1162, 1193 n.8 (10th Cir. 2006).

The Supreme Court has acknowledged the importance of protecting the nation's secrets from disclosure: "The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service." CIA v. Sims, 471 U.S. 159, 175 (1985) (quoting Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam)); accord Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) ("The [executive branch] has available intelligence services whose reports are not and ought not to be published to the world."). Accordingly, federal courts have long recognized that "[i]t is not in the national interest for revelation of either the existence or the product of [foreign intelligence operations and information] to extend beyond the narrowest limits compatible with the assurance that no injustice is done to the criminal defendant." United States v. Lemonakis, 485 F.2d 941, 963 (D.C. Cir. 1973).

#### A. Section 1 – Definitions

For the purposes of CIPA, "classified information" includes any information or material that has been determined by the United States government pursuant to law or regulation to require protection against unauthorized disclosure for reasons of national security. 18 U.S.C.

App. III § 1(a). "National security" means the national defense and foreign relations of the United States. *Id.* § 1(b).

CIPA applies equally to classified testimony and classified documents. *See United States* v. Lee, 90 F. Supp. 2d 1324, 1326 n.1 (D.N.M. 2000) (citing *United States v. North*, 708 F. Supp. 399, 399-400 (D.D.C. 1988)); *Kasi v. Angelone*, 200 F. Supp. 2d 585, 596-97 (E.D. Va. 2002) (applying CIPA to classified testimony).

## B. Section 2 – Pretrial Conference

Section 2 of CIPA—the section the United States is invoking in the instant motion—authorizes the Court, upon motion by any party or at its own discretion, to hold a pretrial conference "to consider matters relating to classified information that may arise in connection with the prosecution." 18 U.S.C. App. III § 2. No substantive issues concerning the use of classified information are to be decided in a Section 2 pretrial conference. *See* S. Rep. No. 96-823, at 5-6, *reprinted in* 1980 U.S.C.C.A.N. 4294, 4298-99 (96th Cong. 2d Sess.).

To foster open discussions at the pretrial conference, Section 2 provides that no admission made by the Defendant or his attorney at the pretrial conference may be used against the Defendant unless the admission is in writing and signed by both the Defendant and his attorney. 18 U.S.C. App. III § 2.

## C. Section 4 – Protection of Classified Information During Discovery

Section 4 of CIPA provides a procedural mechanism to protect classified information, sources, and methods, while simultaneously ensuring that the government is able to satisfy its discovery obligations. CIPA does not create any new right of discovery or expand the rules governing the admissibility of evidence. *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) ("CIPA does not create any discovery rights for the defendant."); *United States v.* 

Johnson, 139 F.3d 1359, 1365 (11th Cir. 1998) ("CIPA has no substantive impact on the admissibility or relevance of probative evidence."); *United States v. Smith*, 780 F.2d 1102, 1106 (4th Cir. 1985) ("The legislative history is clear that Congress did not intend to alter the existing law governing the admissibility of evidence."). Rather, CIPA applies preexisting general discovery law in criminal cases to classified information and restricts discovery of such information to protect the government's national security interests. *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998); *United States v. Baptista-Rodriguez*, 17 F.3d 1354, 1363-64 (11th Cir. 1994); *United States v. Yunis*, 867 F.2d 617, 621 (D.C. Cir. 1989).

CIPA thus does not, and was not intended to, "expand the traditional rules of discovery under which the government is not required to provide criminal defendants with information that is neither exculpatory nor, in some way, helpful to the defense." *United States v. Varca*, 896 F.2d 900, 905 (5th Cir. 1990) (emphasis added); *see United States v. McVeigh*, 923 F. Supp. 1310, 1314 (D. Colo. 1996) ("CIPA does not enlarge the scope of discovery or of *Brady*"). Nor does CIPA provide that the admissibility of classified information be governed by anything other than the "well-established standards set forth in the Federal Rules of Evidence." *Baptista-Rodriguez*, 17 F.3d at 1364.

Accordingly, pursuant to Section 4, district courts have the opportunity to assess whether, and the extent to which, specified items of classified information should be disclosed.

Specifically, Section 4 provides that "[t]he court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting the relevant facts that classified information would tend to prove." 18

U.S.C. App. III § 4; see also United States v. Sedaghaty, 728 F.3d 885, 904 (9th Cir. 2013); United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998).

Similar to Federal Rule of Criminal Procedure 16(d)(1), which gives the district court the authority to "deny, restrict, or defer discovery or inspection, or grant other appropriate relief" for "good cause," Section 4 of CIPA authorizes the district court "upon a sufficient showing" to deny, or otherwise restrict, discovery by the defendant of classified documents and information belonging to the United States. 18 U.S.C. App. III § 4; see, e.g., Rezaq, 134 F.3d at 1142; United States v. Yunis, 867 F.2d 617, 621 (D.C. Cir. 1989). The legislative history of CIPA makes clear that Section 4 was intended to simply clarify the district court's power under Rule 16(d)(1) to deny or restrict discovery in order to protect national security. See S. Rep. No. 96-823, at 6, 1980 U.S.C.C.A.N. at 4299-4300; see also United States v. Aref, 533 F.3d 72, 78-79 (2d Cir. 2008).

CIPA Section 4 also provides, similar to Rule 16(d)(1), that the Government may demonstrate that the use of an alternative discovery procedure—such as deletion or substitution—is warranted. CIPA further specifically provides that the Government may make this showing *in camera* and *ex parte*. 18 U.S.C. App. III § 4; *see United States v. Mejia*, 448 F.3d 436, 457-58 & n.21 (D.C. Cir. 2006) (noting similarity to Federal Rule of Criminal Procedure 16(d)); *see also United States v. Abu-Jihaad*, 630 F.3d 102, 140 (2d Cir. 2010); *Aref*, 533 F.3d at 81; *Yunis*, 867 F.2d at 622-23; *United States v. Pringle*, 751 F.2d 419, 427 (1st Cir. 1985).

### D. <u>Section 7 – Interlocutory Appeal</u>

"[CIPA] permits the government to seek an interlocutory appeal of a district court order authorizing the disclosure of classified information." *United States v. Asgari*, 940 F.3d 188, 189

(6th Cir. 2019). Section 7 permits the United States to take an interlocutory expedited appeal to the appellate court if the Court: (a) authorizes the disclosure of classified information; (b) imposes sanctions for nondisclosure of classified information; or (c) refuses to issue a protective order sought by the United States to prevent the disclosure of classified information. *Id.* § 7. If an appeal is taken, trial shall not commence, or must be adjourned if already commenced, until the appeal is resolved. *Id.* Such an appeal and decision does not affect the defendant's right to lodge a subsequent appeal upon conviction of an adverse ruling by the trial court. *Id.* § 7(b).

## E. Section 8 – Introduction of Classified Information

Section 8 provides in part that, "During the examination in any criminal proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible." 18 U.S.C. App. III § 8. After an objection is made, "the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information." *Id.* Such suitable action may require the Government to provide the Court with a proffer of the witness' response to the question or line of inquiry. *Id.* 

# F. Section 9 – Security Procedures

Section 9 requires the Chief Justice of the United States, in consultation with other executive branch officials, to prescribe rules establishing procedures to protect classified information in the custody of federal courts from unauthorized disclosure. 18 U.S.C. App. III § 9(a). The Chief Justice has done so in the Revised Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of

Classified Information (hereinafter "the Security Procedures").<sup>2</sup> Section 2 of the Security Procedures states:

In any proceeding in a criminal case or appeal therefrom in which classified information is within, or is reasonably expected to be within, the custody of the court, the court will designate a "classified information security officer." The Attorney General or the Department of Justice Security Officer will recommend to the court a person qualified to serve as a classified information security officer. This individual will be selected from the Litigation Security Group, Security and Emergency Planning Staff, Department of Justice, to be detailed to the court to serve in a neutral capacity. The court may designate, as required, one or more alternate classified information security officers who have been recommended in the manner specified above.

## REQUEST FOR PRETRIAL CONFERENCE UNDER CIPA SECTION 2

The Government anticipates that issues regarding the discovery of classified information will arise in this case. Accordingly, the United States respectfully moves for a pretrial conference to consider such matters and establish a motion schedule relating to the classified information pursuant to Section 2 of CIPA.

At the Section 2 pretrial conference, the Government will provide an estimate of the time necessary to complete its review of the classified information. Based on that estimate, the Government will provide a proposed schedule for the filing of motions under CIPA Section 4 relating to the deletion, substitution, or disclosure of classified information. Because of the classified nature of certain information, the Government will be unable to provide the Court with specifics in open court (*e.g.*, the type of information at issue, the amount of information at issue, the period of time when such information was collected, whether agencies other than those involved in the criminal investigation possess relevant information). If the Court so directs, the Government will be prepared to present this information to the Court orally in an *ex parte*, *in* 

 $<sup>^{2}</sup>$  The Security Procedures are included with this Motion as Attachment A.

camera hearing. As previously noted, courts have consistently held that *in camera*, *ex parte* submission to a district court in matters involving national security are proper. *See*, *e.g.*, *Mejia*, 448 F.3d at 455; *United States v. Gurolla*, 333 F.3d 944, 951 (9th Cir. 2003); *Pringle*, 751 F.2d at 427.

#### CONCLUSION

For the reasons discussed above, the United States respectfully requests that the Court grant the motion. The undersigned counsel has conferred with defense counsel about this motion. Counsel for the Defendant indicated that he does not object to this motion.

Respectfully submitted on April 15, 2021.

FRANCIS M. HAMILTON III ACTING UNITED STATES ATTORNEY

By: /s/ Casey T. Arrowood
Casey T. Arrowood
Assistant United States Attorney
TN BPR No. 038225
800 Market Street, Suite 211
Knoxville, TN 37902
(865) 545-4167
Casey.Arrowood2@usdoj.gov

# ATTACHMENT A

# REVISED SECURITY PROCEDURES ESTABLISHED PURSUANT TO PUB. L. 96-456, 94 STAT. 2025, BY THE CHIEF JUSTICE OF THE UNITED STATES FOR THE PROTECTION OF CLASSIFIED INFORMATION

- 1. <u>Purpose</u>. The purpose of these procedures, as revised, is to meet the requirements of Section 9(a) of the Classified Information Procedures Act of 1980, Pub. L. 96-456, 94 Stat. 2025, as amended ("the Act"), which in pertinent part provides that:
- "... [T]he Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. . . ."

These revised procedures apply in all criminal proceedings involving classified information, and appeals therefrom, before the United States district courts, the courts of appeal and the Supreme Court, and supersede the Security Procedures issued on February 12, 1981.

2. <u>Classified Information Security Officer</u>. In any proceeding in a criminal case or appeal therefrom in which classified information is within, or is reasonably expected to be within, the custody of the court, the court will designate a "classified information security officer." The Attorney General or the Department of Justice Security Officer will recommend to the court a person qualified to serve as a classified information security officer. This individual will be selected from the Litigation Security Group, Security and Emergency Planning Staff, Department of Justice, to be detailed to the court to serve in a neutral capacity. The court may designate, as required, one or more alternate classified information security officers who have been recommended in the manner specified above.

The classified information security officer must be an individual with demonstrated competence in security matters. Prior to designation, the Department of Justice Security Officer must certify in writing that the classified information security officer is properly cleared, i.e., possesses the necessary clearance for the level and category of classified information involved.

The classified information security officer will be responsible to the court for the security of all classified information in the court's custody, including, but not limited to, any pleadings or other filings created in connection with the proceedings, and any form of information contained in any format, including testimony, notes, photographs, transcripts, documents, digital files, audio files or video files, stored on any type of equipment (e.g., computers, electronic storage devices, etc.). In addition, any matters relating to personnel, information, or communications security will be the responsibility of the classified information security officer who will take measures reasonably necessary to fulfill these responsibilities. The classified information security officer must notify the court and the Department of Justice Security Officer of any actual, attempted, or potential violation of security procedures.

3. Secure Location. Any in camera proceeding--including, but not limited to, a pretrial conference, motion hearing, status hearing, suppression hearing, substitution hearing, or appellate proceeding--concerning the use, relevance, or admissibility of classified information must be held in a secure location recommended by the classified information security officer and approved by the court.

The secure location must be within the federal courthouse, unless it is determined that no available location in the courthouse meets, or can reasonably be adapted to meet, the security requirements of the Executive Branch applicable to the level and category of classified information involved. In the event that no suitable location exists within the courthouse, upon

recommendation by the classified information security officer, the court will designate another United States Government facility located within the vicinity of the courthouse, as the secure location.

The classified information security officer must make necessary arrangements to ensure that the security requirements of the Executive Branch applicable to the level and category of classified information involved are met and must conduct or arrange for such inspection of the secure location as may be necessary. The classified information security officer must, in consultation with the United States Marshal, arrange for the installation of security devices and take such other measures as may be necessary to protect against any unauthorized access to or disclosure of classified information. All of the aforementioned activities must be conducted in a manner that does not interfere with the orderly proceedings of the court. Prior to any hearing or other proceeding, the classified information security officer must certify to the court that the location to be used is secure.

4. <u>Personnel Security – Court Personnel</u>. No person appointed by the court or designated for service therein will be given access to any classified information in the custody of the court, unless such person has received the appropriate security clearance and unless access to such information is necessary for the performance of an official function. A security clearance for justices and other Article III judges is not required.

The court shall timely notify the classified information security officer of the names of court personnel who may require access to classified information. The classified information security officer will then notify the Department of Justice Security Officer, who will promptly make arrangements to obtain any necessary security clearances. All security clearance requests will be reviewed and determinations will be made in accordance with the adjudication standards

of the Executive Branch applicable to the level and category of classified information involved. The classified information security officer, on behalf of the Department of Justice Security Officer, will advise the court when the necessary security clearances have been obtained. When necessary, the court may request that security clearances for certain court personnel be expedited.

If security clearances cannot be obtained promptly, United States Government personnel possessing the appropriate security clearances may be temporarily assigned to assist the court. If a proceeding is required to be recorded and an official court reporter having the necessary security clearance is unavailable, the court may request the classified information security officer or the attorney for the government to have a cleared reporter designated to act as a reporter in the proceedings. The reporter so designated must take the oath of office as prescribed by 28 U.S.C. § 753(a).

Justices, judges and cleared court personnel may disclose classified information only to persons who possess both the appropriate security clearance and the requisite need to know the information in the performance of an official function. However, nothing contained in these procedures precludes a judge from performing his or her official duties, including giving appropriate instructions to a jury.

Any security concern regarding classified information and involving court personnel or persons acting for the court must be referred to the court and the Department of Justice Security Officer for appropriate action.

5. <u>Persons Acting for the Defense</u>. The government may obtain information by any lawful means concerning the trustworthiness of persons associated with the defense and may

bring such information to the attention of the court for the court's consideration in framing an appropriate protective order pursuant to Section 3 of the Act.

6. <u>Jury</u>. Nothing contained in these procedures will be construed to require an investigation or security clearance of the members of a jury or to interfere with the functions of a jury, including access to classified information introduced as evidence in the trial of a case.

At any time during trial, the trial judge should consider, based on a party request or sua sponte, giving the jury a cautionary instruction regarding the release or disclosure of any classified information provided to the jury.

- 7. Custody and Storage of Classified Materials.
- a. *Materials Covered*. These security procedures apply to any classified information, as the term is defined in Section 1(a) of the Act, that is in the custody of the court. This includes, but is not limited to any pleadings or other filings created in connection with the proceedings, and any form of information contained in any format, such as testimony, notes, photographs, transcripts, documents, digital files, audio files or video files, stored on any type of equipment (e.g., computers, electronic storage devices, etc.).
- b. Safekeeping. Classified information submitted to the court must be placed in the custody of the classified information security officer or appropriately cleared court personnel who will then be responsible for its safekeeping. When not in use, all classified materials must be stored in a safe that conforms to the General Services Administration standards for security containers. Classified information will be segregated from other information unrelated to the case at hand by securing it in a separate security container. If the court does not possess a storage container that meets the required standards, the necessary storage container or containers are to be supplied to the court on a temporary basis by the appropriate Executive Branch agency

as determined by the Department of Justice Security Officer. Only the classified information security officer, alternate classified information security officer(s), and appropriately cleared court personnel will have access to the combination and the contents of the container.

For other than temporary storage (e.g., a brief court recess), the classified information security officer must ensure that the storage area in which these containers will be located meets Executive Branch standards applicable to the level and category of classified information involved. The secure storage area may be located within either the federal courthouse or the facilities of another United States Government agency.

c. Transmittal of Classified Information. During the pendency of any hearing, trial or appeal, classified materials stored in the facilities of another United States Government agency must be transmitted to and from the court in the manner prescribed by the Executive Branch security regulations applicable to the level and category of classified information involved. A trust receipt must accompany all classified materials transmitted and must be signed by the recipient and returned to the classified information security officer.

# 8. Operating Routine.

a. Access to Court Records. Court personnel will have access to court records containing classified information only as authorized. Access to classified information by court personnel will be limited to the minimum number of cleared persons necessary for operational purposes. Access includes presence at any proceeding during which classified information may be disclosed. Arrangements for access to classified information in the custody of the court by court personnel and by persons acting for the defense must be approved in advance by the court, which may issue a protective order concerning such access.

- b. Access to Other Discoverable Information. Except as otherwise authorized by a protective order, persons acting for the defense will not be given custody of classified information provided by the government. They may, at the discretion of the court, be afforded access to classified information provided by the government in secure locations that have been approved in accordance with § 3 of these procedures, but such classified information must remain in the control of the classified information security officer. The classified information security officer also will control access to classified information in the possession of the defense that is filed with the court or is reasonably expected to come within the custody of the court.
- c. *Telephone and Computer Security*. Classified information must not be discussed, communicated, or processed using any non-secure communication device including standard commercial telephone instruments or office intercommunication systems, cellular devices, computers, and/or other electronic or internet-based communication services. Classified information may only be discussed, communicated and processed on devices cleared for the level of classification of the information to be disclosed or processed as approved by the Classified Information Security Officer.
- d. *Disposal of Classified Material*. The classified information security officer is responsible for the secure disposal of all classified materials in the custody of the court which are not otherwise required to be retained.

### 9. Records Security.

a. *Classification Markings*. The classified information security officer, after consultation with the appropriate classification authority, is responsible for marking all court materials containing classified information with the appropriate level of classification, and for indicating

thereon any special access controls that also appear on the face of the material from which the classified information was obtained or that are otherwise applicable.

Any and all materials potentially containing classified information filed by the defense must be filed under seal with the classified information security officer. The classified information security officer may permit counsel to file, on the public docket, non-substantive pleadings or documents (e.g., motions for extension of time, scheduling matters, continuances, etc.) that do not contain information that is or may be classified. The classified information security officer must promptly coordinate with the appropriate classification authority to determine whether each filing contains classified information. If it is determined that the filed material does contain classified information, the classified information security officer must ensure that it is marked with the appropriate classification markings. If it is determined that the filed material does not contain classified information, it should be unsealed and placed in the public record. Upon the request of the government, the court may direct that any filed materials containing classified information must thereafter be maintained in accordance with § 7 of these procedures.

b. Accountability System. The classified information security officer is responsible for the establishment and maintenance of a control and accountability system for all classified information received by or transmitted from the court. Upon request, the classified information security officer will provide to the court an inventory of all classified information received by the court.

10. <u>Transmittal of the Record on Appeal</u>. The record on appeal, or any portion thereof, which contains classified information must be transmitted to the court of appeals or to the Supreme Court in the manner specified in § 7(c) of these procedures.

Any court records containing classified information must be maintained, through the pendency of any direct appeal, at a secure location that is reasonably accessible and approved by the classified information security officer, and must be stored in a proper security container.

- 11. <u>Final Disposition</u>. Within a reasonable time after all proceedings in the case have been concluded, including appeals, the court will release to the classified information security officer all materials containing classified information. The classified information security officer will then transmit them to the Department of Justice Security Officer to be maintained in accordance with approved storage procedures. The materials must be transmitted in the manner specified in § 7(c) of these procedures and must be accompanied by the appropriate accountability records required by § 9(b) of these procedures.
- 12. <u>Expenses</u>. All expenses of the United States Government that arise in connection with the implementation of these procedures, including any construction or equipment costs, will be borne by the Department of Justice and other appropriate Executive Branch agencies whose classified information is being protected.
- 13. <u>Interpretation</u>. Any question concerning the interpretation of any security requirement contained in these procedures will be resolved by the court in consultation with the Classified Information Security Officer who will consult with the Department of Justice Security Officer, if necessary.
- 14. <u>Term</u>. These revised procedures remain in effect until modified in writing by The Chief Justice after consultation with the Attorney General of the United States, the Director of National Intelligence, and the Secretary of Defense.
- 15. <u>Effective Date</u>. These revised procedures become effective forty-five days after the date of submission to the appropriate Congressional Committees, as required by the Act.

Effective this 15th day of January, 2011, having taken into account the views of the Attorney General of the United States, the Director of National Intelligence, and the Secretary of Defense, as required by law.

[The revised security procedures set out above were issued Dec. 1, 2010, by John G. Roberts, Jr., Chief Justice of the United States. Prior security procedures were issued Feb. 12, 1981, by Warren E. Burger, Chief Justice of the United States.]